## 21.5 Cyclotomic Polynomials

In order to fill in the technical gap we first need:

***THEOREM 21.4***
*Any two primitive nth roots of unity in $\mathbb{C}$ have the same minimal polynomial over $\mathbb{Q}$.*

Before starting on the proof, some motivation will be useful. Consider the case $n = 12$. Let

$$\zeta = \zeta_{12} = \cos\frac{2\pi}{12} + i\sin\frac{2\pi}{12}$$

We can classify the $\zeta^j$ according to their minimal power $d$ such that $\zeta^d = 1$. That is, we consider when they are *primitive* $d$th roots of unity. It is easy to see that in this case the primitive $d$th roots of unity are:

$$\begin{array}{ll} d = 1 & 1 \\ d = 2 & \zeta^6 (= -1) \\ d = 3 & \zeta^4, \zeta^8 (= \omega, \omega^2) \\ d = 4 & \zeta^3, \zeta^9 (= i, -i) \\ d = 6 & \zeta^2, \zeta^{10} (= -\omega, -\omega^2) \\ d = 12 & \zeta, \zeta^5, \zeta^7, \zeta^{11} \end{array}$$

We can factorize $t^{12} - 1$ by grouping corresponding zeros:

$$\begin{aligned} t^{12} - 1 = {} & (t-1)\times \\ & (t-\zeta^6)\times \\ & (t-\zeta^4)(t-\zeta^8)\times \\ & (t-\zeta^3)(t-\zeta^9)\times \\ & (t-\zeta^2)(t-\zeta^{10})\times \\ & (t-\zeta)(t-\zeta^5)(t-\zeta^7)(t-\zeta^{11}) \end{aligned}$$

which simplifies to

$$t^{12} - 1 = (t-1)(t+1)(t^2+t+1)(t^2+1)(t^2-t+1)F(t)$$

where

$$F(t) = (t-\zeta)(t-\zeta^5)(t-\zeta^7)(t-\zeta^{11})$$

whose explicit form is not immediately obvious. One way to work out $F(t)$ is to use trigonometry (Exercise 21.4). The other is to divide $t^{12} - 1$ by all the other factors, which leads rapidly to

$$F(t) = t^4 - t^2 + 1$$



If we let $\Phi_d(t)$ be the factor corresponding to primitive $d$th roots of unity, we have proved that

$$t^{12} - 1 = \Phi_1\Phi_2\Phi_3\Phi_4\Phi_6\Phi_{12}$$

Our computations show that every factor $\Phi_j$ lies in $\mathbb{Z}[t]$. In fact, it turns out that the factors are all *irreducible* over $\mathbb{Z}$. This is obvious in some cases, and follows by the usual trick with Eisenstein's Criterion in the others (Exercise 21.11). This calculation generalizes, as the following proof (eventually) shows.

**PROOF OF THEOREM 4** Let $J = J_n$ be the set of all $n$th roots of unity in $\mathbb{C}$, primitive or not. Define a relation $\sim$ on $J$ by

$$\varepsilon \sim \delta \Leftrightarrow m_\varepsilon(t) = m_\delta(t)$$

where $m_\varepsilon(t)$ is the mimimum polynomial of $\varepsilon$ over $\mathbb{Q}$, and similarly for $m_\delta(t)$. It is clear that $\sim$ is an equivalence relation, so it partitions $J$ into equivalence classes. Let $[\varepsilon]$ denote the equivalence class of $\varepsilon \in J$.

Over $\mathbb{C}$ there is a factorization

$$t^n - 1 = \prod_{\delta\in J}(t-\delta)$$

and $m_\varepsilon(t) | t^n - 1$ and is monic, so we must have

$$m_\varepsilon(t) = \prod_{\delta\in K_\varepsilon}(t-\delta)$$

for some subset $K_\varepsilon \subseteq J$.

Over $\mathbb{C}$, the linear polynomial $t - \varepsilon$ divides $m_\varepsilon(t)$, hence $t - \delta$ divides $m_\varepsilon(t)$ for all $\delta \sim \varepsilon$. Therefore, the equivalence class $[\varepsilon]$ of $\varepsilon$ is contained in $K_\varepsilon$. In fact, these sets must be equal, for if $K_\varepsilon$ contains any $\delta \not\sim \varepsilon$, then both $m_\varepsilon(t)$ and $m_\delta(t)$ are divisible by $t - \delta$. Since $\delta \not\sim \varepsilon$ these polynomials are coprime over $\mathbb{Q}$, because they are distinct monic irreducibles over $\mathbb{Q}$, so there exist $a(t), b(t) \in \mathbb{Q}[t]$ such that

$$a(t)m_\varepsilon(t) + b(t)m_\delta(t) = 1$$

Then $t - \delta$ divides $a(t)m_\varepsilon(t) + b(t)m_\delta(t)$ over $\mathbb{C}$, but this is 1, a contradiction.

We have, therefore, proved that

$$m_\varepsilon(t) = \prod_{\delta\in K_\varepsilon}(t-\delta) = m_{[\varepsilon]}(t)$$

say. Since the equivalence classes partition $J$,

$$t^n - 1 = \prod_{[\varepsilon]} m_{[\varepsilon]}(t) \qquad (21.10)$$

where the $m_{[\varepsilon]}(t)$ are monic irreducible polynomials over $\mathbb{Q}$. Thus (21.10) is the factorization of $t^n - 1$ into monic irreducibles over $\mathbb{Q}$, hence also (by Corollary 3.18 to Gauss's Lemma) the factorization of $t^n - 1$ into monic irreducibles over $\mathbb{Z}$. In particular, each $m_{[\varepsilon]}(t)$ lies in $\mathbb{Z}[t]$.

We claim that if $p$ is any prime that does not divide $n$, and $\varepsilon \in J$, then $\varepsilon \sim \varepsilon^p$. This step, which is not at all obvious, is the heart of the proof.

We prove the claim by contradiction. If it is false, then $m_{[\varepsilon^p]}(t) \neq m_{[\varepsilon]}(t)$. Define

$$k(t) = m_{[\varepsilon^p]}(t^p) \in \mathbb{Z}[t]$$

so

$$k(\varepsilon) = m_{[\varepsilon^p]}(\varepsilon^p) = 0$$

Therefore, $m_{[\varepsilon]}(t)$ divides $k(t)$ in $\mathbb{Z}[t]$, so there exists $q(t) \in \mathbb{Z}[t]$ such that

$$m_{[\varepsilon]}(t)q(t) = k(t)$$

Reduce coefficients modulo $p$ as in Section 3.5. Using bars to denote images modulo $p$,

$$\bar{m}_{[\varepsilon]}(t)\bar{q}(t) = \bar{k}(t) = \bar{m}_{[\varepsilon^p]}(t^p) = \left(\bar{m}_{[\varepsilon^p](t)}\right)^p$$

since the Frobenius map is a monomorphism in characteristic $p$ by Lemma 17.14. Therefore, $\bar{m}_{[\varepsilon^p](t)}$ and $\bar{m}_{[\varepsilon](t)}$ have a common zero in some extension field of $\mathbb{Z}_p$, so that

$$\overline{t^n - 1} = \prod_{[\varepsilon]} \bar{m}_{[\varepsilon]}(t)$$

has a repeated zero in some extension field of $\mathbb{Z}_p$. By Lemma 9.13 (generalized), $\overline{t^n - 1}$ and its formal derivative have a common zero. However, the formal derivative of $\overline{t^n - 1}$ is $\bar{n}t^{n-1}$ and $\bar{n} \neq 0$ since $p \nmid n$. Now

$$\frac{t}{\bar{n}}(\bar{n}t^{n-1}) - \overline{t^n - 1} = \bar{1}$$

so no such common zero exists (that is, $\bar{n}t^{n-1}$ and $\overline{t^n - 1}$ are coprime). This contradiction shows that $\varepsilon^p \sim \varepsilon$.

It follows that $\varepsilon^u \sim \varepsilon$ for every $u = p_1 \dots p_l$ where the $p_j$ are primes not dividing $n$. These $u$ are precisely the natural numbers that are prime to $n$, so modulo $n$ they form the group of units $\mathbb{Z}_n^*$.

For each divisor $d$ of $n$, let $J_d \subseteq J$ be the set of all *primitive* $d$th roots of unity. Then

$$J = \dot{\bigcup}_{d|n} J_d$$

where $\dot{\bigcup}$ indicates that the union is disjoint. Clearly,

$$J_d = \{\varepsilon^u : u \in \mathbb{Z}_n^*\}$$



for any $\varepsilon \in J_d$, because $p \nmid n$ implies $p \nmid \frac{n}{d}$. Therefore, if $\varepsilon$ is a primitive $d$th root of unity, $J_d \subseteq [\varepsilon]$. Thus if $\varepsilon, \delta$ are any two primitive $d$th roots of unity, then $[\varepsilon] \cap [\delta] \neq \emptyset$. But equivalence classes are either equal or disjoint, so we have a contradiction. Therefore, $J_d = [\varepsilon]$ for any $\varepsilon$ that is a primitive $d$th root of unity.

We deduce that

$$\Phi_d(t) = \prod_{\sigma \in J_d} (t - \sigma)$$

is the minimal polynomial of *any* primitive $d$th root of unity. Therefore, any two primitive $d$th roots of unity have the same minimal polynomial, namely, $\Phi_d(t)$, as required. □

***DEFINITION 21.5*** *The polynomial $\Phi_d(t)$ is the $d$th* cyclotomic polynomial *over* $\mathbb{C}$.

***COROLLARY 21.6***
*For all $d \in \mathbb{N}$, the polynomial $\Phi_d(t)$ lies in $\mathbb{Z}[t]$ and is monic and irreducible.*

---

## 21.6 The Technical Lemma

We can now fill in the technical gap in the proof of the Vandermonde-Gauss Theorem in Section 21.4.

***THEOREM 21.7***
*Let $K$ be the splitting field of $\Phi_n(t)$ over $\mathbb{Q}$. Then the Galois group of the extension $K : \mathbb{Q}$ is isomorphic to the group of units $\mathbb{Z}_n^*$ of the ring $\mathbb{Z}_n$.*

**PROOF** The zeros of $\Phi_n(t)$ in $\mathbb{C}$ are powers $\zeta^a$ of a primitive $n$th root of unity $\zeta$, where $a$ ranges through the integers modulo $n$ that are prime to $n$.

Let $\sigma \in \Gamma(K : \mathbb{Q})$. The effect of $\sigma$ is uniquely determine by $\sigma(\zeta)$, and both $\zeta$ and $\sigma(\zeta)$ must have the same minimal polynomial over $\mathbb{Q}$, namely, $\Phi_n(t)$. Therefore, $\sigma(\zeta) = \zeta^a$, where $a \in \mathbb{Z}_n^*$.

Let $\sigma_a$ be the map determined by a given $a \in \mathbb{Z}_n^*$. By Proposition 11.4 (generalized), $\sigma_a$ is a $\mathbb{Q}$-automorphism of $K$, hence lies in the Galois group. Therefore, $\Gamma(K : \mathbb{Q})$ consists of precisely the maps $\sigma_a$ for $a \in \mathbb{Z}_n^*$. Now

$$\sigma_a(\sigma_b(\zeta)) = (\zeta^b)^a = \zeta^{ab}$$

so the map $\sigma_a \mapsto a$ is an isomorphism between $\Gamma(K : \mathbb{Q})$ and $\mathbb{Z}_n^*$. □